
HOT TOPICS II: INTERNET SAFETY AND ETHICS



INTERNET SAFETY

- Today there are many issues relevant to Internet safety such as:
 - ❑ Privacy
 - ❑ Misinformation
 - ❑ Malware
-

WHAT IS PRIVACY?

- The claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others
- Another definition is:
 - “the condition of having *control* over information about oneself.”
 - “Privacy consists in having control over how much and what kind of information about oneself is given to others.”

THE FBI AND DATA QUALITY

- Kenneth Laudon, *Data Quality and Due Process in Large Inter Organizational Record Systems*, CACM Jan 1986.
 - 250 million criminal history records are maintained by the FBI and available to local law persons "on the beat".
 - Methodology:
 - sampled records in NCIC-CCH (computerized criminal history) files and the wanted persons/ outstanding warrant files.
 - compared online info to the original, paper based files at the point where the arrest occurred.
-

FBI DATA QUALITY: RESULTS AND PROBLEMS

■ Results

- ❑ Complete, accurate and unambiguous records: 46%
- ❑ No disposition/ incomplete records: 28%
- ❑ Inaccurate records: 17%
- ❑ Ambiguous or combined problems: 9%

■ Problems—Files are used by:

- ❑ police when doing a "stop and search"
 - ❑ prospective employers (more often than police!)
 - ❑ judges in setting bail
-

WHAT IS AT STAKE?

- What do we stand to lose along with our privacy?
 - ❑ Freedom from intrusion into our personal “space”
 - ❑ Freedom from surveillance
 - ❑ Freedom to act as we choose
 - ❑ Time, money, and other resources
 - ❑ Our lives
-

WHAT'S THE BIG DEAL?

- People have been collecting personal information for millennia. Why is privacy such a concern all of a sudden?
- Computers change:
 - The scale of information gathering
 - The types of information that is gathered
 - The scale of information distribution and exchange
 - The effect or magnitude of impact of erroneous data
 - The length of time that the info endures

DATA, DATA, EVERYWHERE

- **Government Databases**—on average you are in about 20 government databases:
 - ❑ Birth Marriage and Death data
 - ❑ Educational records (Schools, including psychological testing results)
 - ❑ Police (arrests, convictions, warrants, etc.)
 - ❑ IRS (earnings, taxes)
 - ❑ Motor vehicles (ownership, accidents)
 - ❑ Books checked out of libraries
 - ❑ Medical records covered by Medicare or armed services
 - ❑ National Security - Informants, potential agents, Military records etc.
 - ❑ Welfare (social security, unemployment, veteran's benefits, etc.)
 - ❑ Voter registration
 - ❑ Relocation and address change (post office)

DATA, DATA, EVERYWHERE

■ **Private/Corporate databases:**

- ❑ Financial (banks, credit cards, loans, purchases)
 - ❑ Medical records (insurance companies)
 - ❑ Subscription and membership lists
 - ❑ Video rental records, books purchased, telephone records
 - ❑ Employment files, airline travel records
-

WHO HAS ACCESS? EVERYONE.

- Regulation shmeregulation!
- In the US at present, anybody can sell any information:
 - ❑ Patients who have sued their doctors for malpractice
 - ❑ Tenants who have sued landlords

The screenshot shows the PeopleFind.com website in a Microsoft Internet Explorer browser window. The browser's address bar shows "PeopleFind.com - Microsoft Internet Explorer". The page has a blue header with the 411.COM logo in the center. On the left, there's a section titled "NEXT DAY RESULTS!" with a small photo of a couple. On the right, there's a section titled "FIND ANYONE!" with a small photo of two children. Below the header, there's a blue banner with the text "LOCATE ANYONE! Next Day Search Results: Internet Special! \$39.95". The main content area is divided into two columns. The left column has the text "Looking for a long lost love, an old friend, or a family member? To locate someone, all you need is their Name and one of the following:" followed by a list of search criteria: "Previous Address OR Date of Birth OR Social Security Number OR Possible State of Residence". The right column has the text "Click here to find out what you get in the person locator report" and "If you only have a Name to go on, click here for more options." Below this, there's a "Secure Order Form" button. The bottom section of the page is titled "BACKGROUND CHECKS! Next Day Results: Internet Special! \$69.95". It contains the text "Be Informed, Be Safe: Conduct a background check and know beforehand who you let into your home or office!" and "Click here to find out what you get in the background report". To the right, there's a photo of a man and a woman, and the text "To conduct a background check on someone, all you need is their Name and one of the following:" followed by a list of search criteria: "Present/Previous Address OR Date of Birth OR Social Security Number". At the bottom, there are two blue buttons: "ALIVE or DECEASED? - \$24.95!" and "CRIMINAL RECORDS - \$29.95!".

PERSONAL PRIVACY ACT OF 1974

- The purpose of this act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring federal agencies, except as otherwise provided by law to:
 1. Publish a notice of their record systems in the Federal database, so the public can be informed about what exists
 2. Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent
 3. Permit an individual to gain access to information pertaining to him in federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records
 4. Permit **exemptions from the requirements** with respect to records provided in this act only in those cases where there is an important public policy need for such exemptions as has been determined by specific statutory authority, including: **law enforcement, national security**

MISINFORMATION

- With the huge volume of information in the Internet it is very easy to be misled
 - This could potentially lead you to viruses, spyware, scams, illegal sites, etc.
 - Consider the source of information and the bias of information providers
 - Develop a “healthy skepticism”
-

EVALUATING INFORMATION SOURCES

- Where does it come from?
 - Friends/Family
 - Instructors/respected authorities/experts
 - News (papers, TV, radio, online)
 - Websites
 - Corporate
 - Blogs
 - Online Community/Forum
 - Referred (scientific) journals
-

EVALUATING MOTIVES

- Why is this person telling me this?
 - Personal gain: hidden or explicit
 - To be helpful
 - Out of necessity
 - Altruism/Higher purpose, e.g. pursuit of knowledge
 - Why is this person telling me this *now*?
 - Timing of product updates or news
-

EVALUATING METHODOLOGY

- How was this information gathered?
 - ❑ Hearsay or rumor
 - ❑ Opinion (not necessarily based on “fact”)
 - ❑ Hastily, e.g. news tries to get the “scoop”
 - ❑ By an individual or a group?
 - ❑ Through open channels or private?
 - ❑ Explicit methodology or unstated?
-

EVALUATING CONTENT

- Does the information make sense? Why do/don't you believe it?
 - The evidence presented
 - Correlation with past experience/other information sources
 - Your own competence/expertise in this area of information
 - Logical and/or methodological rigor
 - *You may have to dig deeper to really understand this information*
-

MALWARE

- It is malicious software designed to infiltrate or damage a computer system without the owner's informed consent.
 - The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.
 - *Some common examples are viruses, worms, rootkits, spyware.*
-

MALWARE

■ Computer Virus

- ❑ It is a block of code that inserts copies of itself into other programs.
- ❑ It generally carries a payload, which may have nuisance value, or serious consequences.
- ❑ To avoid early detection, viruses may delay the performance of functions other than replication.

■ Worm

- ❑ It is a program that propagates copies of itself over networks harming them by consuming bandwidth.
- ❑ It does not infect other programs.

■ Exploit

- ❑ It is an established way of performing an attack on a vulnerability
- ❑ Standard techniques are supported by established guidelines and programming code, which circulate on the Internet.
- ❑ Code that enables easy performance of an exploit is expressed in a script

MALWARE

■ Spyware

- Software that surreptitiously gathers data within a device (e.g. about its user), or the uses made of it and makes it available to some other party without users consent.

■ Phishing

- Act of fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication

■ Rootkit

- Set of software tools intended to conceal running processes, files or system data from the operating system.
 - Often modify parts of the operating system or install themselves as drivers or kernel modules.
 - Help intruders maintain access to systems while avoiding detection
-

FIGHTING MALWARE

- Dealing with malware can be done by getting software that removes it:
 - ❑ **Viruses and Worms:** McAfee Viruscan, Norton Antivirus, AVG (free).
 - ❑ **Exploits:** install latest patches and upgrades for your operating system and major software.
 - ❑ **Spyware:** Spy Sweeper, Spybot (free)
 - ❑ **Phishing:** McAfee Site Advisor (part of McAfee Security Center), Internet Explorer 7 with phishing filter active (free)
 - ❑ **Rootkits:** AVG (also checks for rootkits -- free)
 - Individual software or an entire suit may be obtained to deal with it.
 - Just remember that if you acquire a suit, make sure you are clear **what type of malware it deals with.**
-

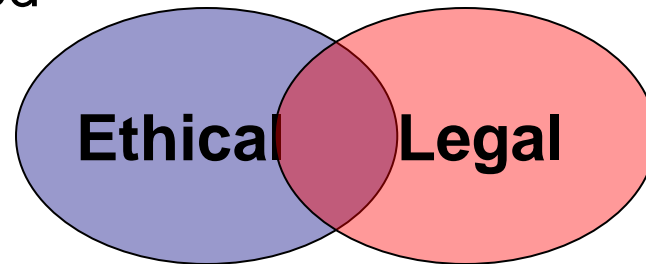
ETHICS

■ Definition

- ❑ Ethics is about making good **decisions** regarding “right” and “wrong,” “good” and “bad”
- ❑ Ethics is about discovering standards for behavior

■ Ethical ≠ Legal

- ❑ Sometimes things that are legal are not ethical, e.g. slavery
- ❑ Sometimes things that are ethical are not legal, e.g. medical marijuana use.
- ❑ Laws do not exist covering every type of behavior, but ethics can **always** be applied



ETHICS IN COMPUTING

- The following is an example of an ethics code for computer professionals:
 1. Contribute To Society And Human Well-being
 - The products of their efforts will be used in socially responsible ways,
 - Will meet social needs, and
 - Will avoid harmful effects to health and welfare (loss of info., property loss or damage, etc.)
 2. Avoid harm to others
 3. Be honest and trustworthy
 4. Be Fair And Take Action Not To Discriminate
-

ETHICS IN COMPUTING

5. Honor Property Rights Including Copyrights And Patents
 6. Respect The Privacy Of Others
 - only the necessary amount of personal information be collected in a system,
 - retention and disposal periods for that information be clearly defined and enforced
 - personal information gathered for a specific purpose is not to be used for other purposes without consent of the individual(s).
 7. Honor Confidentiality
 - With respect to clients, employers, users, co-workers, other professionals.
 - As a professional you will be forced to make decisions that may hurt people, but codes of ethics are a useful guides to your behavior.
-

ETHICAL ANALYSIS

- This type of analysis can help deal with ethical issues and consist of nine steps phrased as questions:
 1. Who is the **moral agent**?
 2. What thing(s) of value is at stake?
 3. Who are the (major) **stakeholders**?
 4. What are the **main courses of action**?
 5. What are the probable **consequences** of each action on each set of stakeholders?
 6. How does utilitarian theory apply?
 7. How does deontological theory apply?
 8. What do relevant codes of ethics indicate?
 9. Finally, what concrete action do you recommend?

STEP 1: WHO IS THE MORAL AGENT?

- An *agent* is someone or something capable of making decisions.
 - *Moral* implies:
 - The ability to tell “right” from “wrong”
 - Responsibility/culpability for one’s action
 - May be an individual or a group.
 - Is the person or persons ultimately responsible for choosing a concrete action, and who will **bear the blame** or responsibility for that action
-

STEP 2: WHAT ARE THE STAKES?

- Something of value *always* is at risk
 - Tangible items:
 - Money
 - Property
 - Life/health
 - Intangible items:
 - Privacy
 - Freedom/liberty
 - Time
 - Comfort/peace of mind
-

STEP 3: WHO STANDS TO GAIN AND LOSE?

- *Stakeholders* are the people or groups who stand to get or lose something of value.
 - Almost always includes the moral agent.
 - Stakeholders may or may not have any influence on the decision made by the moral agent.
 - Be realistic: beware of “the general public” or “everyone in the world”.
-

STEP 4: WHAT TO DO? (MAIN COURSES OF ACTION)

- Most every ethical dilemma boils down to between 2 and 4 possible options.
 - Warning: given enough time you can dream up 100's of 'flavors' of action.
 - However, you *don't* have lots of time.
 - Keep it simple—only analyze the most obvious courses of action.
 - In this step: DO NOT discuss possible outcomes at all.
-

STEP 5: MATRIX OF OUTCOMES

- #stakeholders x #options = #outcomes
 - Lots of stakeholders combined with lots of options makes for impossibly complex and lengthy analysis.
 - Predicting the future is uncertain
 - Focus on the most **probable** outcomes.
 - Strive for balance
 - *Realistic* list of stakeholders
 - *Realistic* list of courses of action
-

STEP 6: THE POWER OF UTILITARIAN THEORY

- Utilitarian theory basic postulates:
 - ❑ Ultimately everyone wants to be “happy”
 - ❑ Right action maximizes happiness
 - ❑ “Good” or “Bad” is entirely determined by the **consequences** of one’s action.
- “right action” maximizes the positive outcomes for the greatest number of people.
- Important tensions:
 - ❑ Short term vs. Long term consequences
 - ❑ Predictability/probability of outcomes
 - ❑ Rule vs. Act utilitarianism (universal rules of behavior vs. no rules, case by case analysis)

STEP 7: THE POWER OF DEONTOLOGY

- Deontology theory basic postulates:
 - Goodness is **not** a calculation of probable consequences
 - What's right is based upon your 'duty,' and can be determined *a priori* (i.e. before you act)
- Key Questions:
 - What is your duty in this case?
 - What rules apply?
- "Duty" comprises a set of written and unwritten moral obligations to others, e.g. self, family, society, environment and consequences are NOT a factor.
- Important tensions:
 - Conflict of duties—e.g. self vs. company
 - Self-sacrifice in the name of duty
 - Society frequently doesn't reward the "honorable" choice, e.g. lack of protection for whistle-blowers

STEP 8: REFERRING TO CODES OF ETHICS

- Written rules of one's profession.
- Clear guidelines for behavior.
- Authority/Legitimacy based upon:
 - Broad, participatory development by members of the field, especially 'elders'
 - Longevity—standing the 'test of time'
 - Clear statement of concern for the well-being of society—i.e. difficult to contradict
- Downsides:
 - Not generally legally binding
 - Do not provide airtight legal protection

STEP 9: YOU *MUST* DO SOMETHING

- At the end of the day, you ***have to*** make a choice.
 - Sometimes it's easy: utilitarian theory, deontology, and codes of ethics frequently agree.
 - If things “work out okay” no one will question *why* you made the choice you did.
 - BUT, if things go badly, you need to be able to defend your choice.
 - Following the process outlined here can help minimize the consequences of a poor choice.
-

ETHICS CONCLUSION

- Bad choices hurt people.
 - Indifference to pain is not professional.
 - Sometimes causing harm is inevitable.
 - The most difficult choices involve deciding who to hurt more.
 - Choices generally get harder the higher up you go in an organization.
 - Lack of direct personal consequences is **NOT** an excuse for unethical behavior.
-